Stability analysis of token-based wireless networked control systems under deception attacks

Article (Accepted Version)

Stability Analysis of Token-based Wireless Networked Control Systems under Deception Attacks

Dajun Du[a], Changda Zhang[a,*], Haikuan Wang[a], Xue Li[a], Huosheng Hu[b], Taicheng Yang[c]

[a]*Shanghai Key Laboratory of Power Station Automation Technology, School of Mechatronic Engineering and Automation, Shanghai University, Shanghai 200072, P.R. China*

[b]*Department of Computer Science, University of Essex, Wivenhoe Park, Colchester CO3 4SQ, UK*

[c]*Department of Engineering and Design, University of Sussex, Brighton BN1 9QT, UK*

Abstract

Currently cyber-security has attracted a lot of attention, in particular in wireless industrial control networks (WICNs). In this paper, the stability of wireless networked control systems (WNCSs) under deception attacks is studied with a token-based protocol applied to the data link layer (DLL) of WICNS. Since deception attacks cause the stability problem of WNCSs by changing the data transmitted over wireless network, it is important to detect deception attacks, discard the injected false data and compensate for the missing data (i.e., the discarded original data with the injected false data). The main contributions of this paper are: 1) With respect to the character of the token-based protocol, a switched system model is developed. Different from the traditional switched system where the number of subsystems is fixed, in our new model this number will be changed under deception attacks. 2) For this model, a new Kalman filter (KF) is developed for the purpose of attack detection and the missing data reconstruction. 3) For the given linear feedback WNCSs, when the noise level is below a threshold derived in this paper, the maximum allowable duration of deception attacks is obtained to maintain the exponential stability of the system. Finally, a numerical example based on a linearized model of an inverted pendulum is provided to

*Corresponding author. Tel.: +086-021-56331634.
Email address: silenceupdown@hotmail.com (Changda Zhang).

demonstrate the proposed design.

Keywords: Deception attacks, Token-based protocol, Kalman filter, Wireless networked control systems, Switched systems

1. Introduction

Industrial wireless network has been increasingly employed in many automation fields to form wireless networked control systems (WNCSs), such as cooperative automated vehicles and unmanned aerial vehicles [6, 28, 29, 33, 41], due to their low cost, flexibility, scalability and easy deployment [11, 12, 36, 39]. They are connected with smart sensors and actuators distributed in various geographical places and communicated with the controllers over multiple wireless channels. A number of research issues, such as communication protocols, fault diagnosis and distributed control, have been extensively investigated to enable their successful operations [9, 40].

WNCSs have been found vulnerable to cyber attacks as they are deployed in a large scale of real world applications over unencrypted cyber communication environments [21, 26]. As large amounts of data from distributed sensors need to be exchanged timely over wireless network, these cyber attacks may trigger the severe faults of WNCSs due to their deep integration of communication and control. Therefore, the cyber-security of WNCSs is an important and urgent problem, which has attracted great interests from both academia and industry.

Deception attacks are one type of the most popular cyber attacks, which may pose potentially significant threats to WNCSs by breaking into the radio range of the wireless nodes for the purpose of injecting the predesigned false data into the measurements. An adversary can usually make these attacks by distorting, replaying or replacing data packets to destroy the authenticity of measurement data [1, 7, 8, 10], and it has stimulated several research works. For example, a malicious cyber attack strategy is designed for wireless network to handle the false data detected by the remote state estimator [19], and the optimal malicious attack strategies to achieve the bound of performance degradation are presented in [3].

Furthermore, to defend wireless network against deception attacks, the state estimator with an event-triggered scheme and the sufficient condition to guarantee the system convergence are proposed in [42]. For perturbation in the control loop by compromising a subset of sensors and injecting an ex-

ogenous control input, the whole system is modelled as a constrained control system and the maximum perturbation is given in the form of reachable set computation [27]. Under deception attacks, an intrusion detection system is designed for WNCSs to identify the existence of the attacks.

These aforementioned works are mainly focused on the design and detection of deception attacks in wireless network. However, since different topological structures are deployed in wireless network, the corresponding communication characters are different [16, 17, 20, 30–32, 37]. This paper is mainly concerned with token-based WNCSs under deception attacks. The token-based wireless network consists of many wireless nodes, where a wireless node is treated as a master station and other nodes are regarded as slave stations. The data exchange between master and slave stations is controlled by using the tokens, which may be injected with the false data, leading to the deterioration of the system performance or even system instability. Therefore, we face the following new challenges and difficulties:

1) The first challenge is how to model the closed-loop system based on the traditional switched system. The difficulty is that the switching character introduced by the token-based protocol to the closed-loop system aggravates the complexity of system modelling.

2) When deception attacks destroy the authenticity of measurement data and the integrity of the token-based industrial wireless network, how to design a new KF to detect deception attacks and reconstruct the missing data is the second challenge.

3) The third challenge is how to analyze the maximum allowable duration of deception attacks to maintain the exponential stability of the system considering the switching character of the closed-loop system.

This paper investigates the stability of token-based WNCSs under deception attacks. The main contributions include: 1) An innovative switched system model is developed with the varying number of the sub-systems for deception attacks. 2) A new KF is developed for attack detection and the missing data reconstruction. 3) The maximum allowable duration of deception attacks is obtained for guaranteeing the exponential stability of the system.

The reminder of this paper is organized as follows. Section 2 describes the problem formulation, including the character analysis of token-based WNCSs, synergic action within deception attacks detection and control center

(DADCC) as well as control objectives. The stability analysis is given in Section 3 and simulation results are provided in Section 4, followed by the conclusion in Section 5.

2. Problem formulation

2.1. The character analysis of token-based WNCSs

Fig. 1 shows the structure of token-based WNCSs, where the outputs of the system are sampled by the distributed sensors and transmitted via a token-based WICN. The data transmission through wireless network may be under deception attacks, which can be detected in the DADCC by using a KF. Furthermore, according to the detection results, the missing data are compensated and the control signals are finally produced.

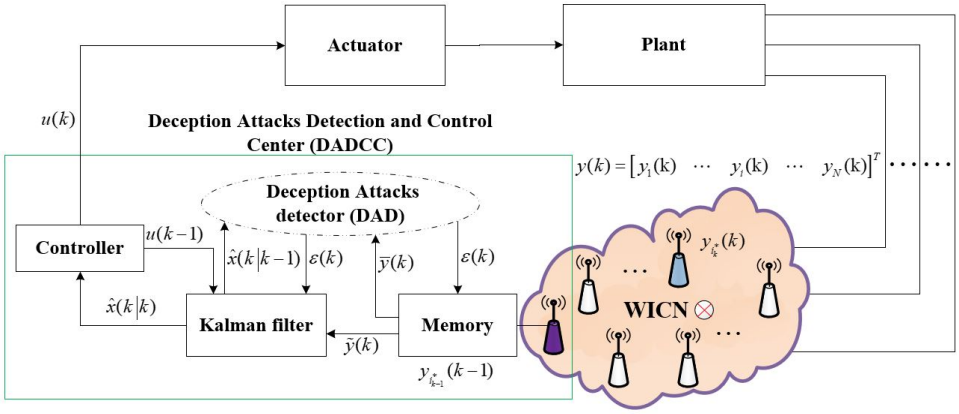

Fig. 1. The scheme of token-based WNCSs.

Consider the following plant:

$$x(k+1) = Ax(k) + Bu(k) + w(k), \tag{1}$$

$$y(k) = Cx(k) + v(k), \tag{2}$$

where $x(k) \in \mathbb{R}^{n_x}$ and $u(k) \in \mathbb{R}^{n_u}$ are the state vector and the control input vector; $y(k) = [y_1(k) \dots y_i(k) \dots y_N(k)]^T \in \mathbb{R}^N$ are the measurement outputs; $w(k) \in \mathbb{R}^{n_x}$ and $v(k) \in \mathbb{R}^N$ are the process noise and the measurement noise with zero mean as well as covariance matrices $Q \in \mathbb{R}^{n_x \times n_x}$ and $R \in \mathbb{R}^{N \times N}$,

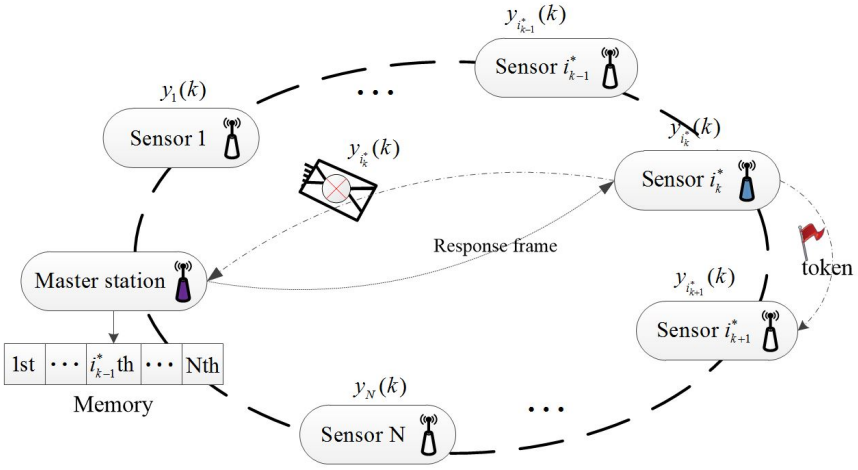

Fig. 2. The topological structure of the WICN.

respectively; $A \in \mathbb{R}^{n_x \times n_x}$, $B \in \mathbb{R}^{n_x \times n_u}$ and $C \in \mathbb{R}^{N \times n_x}$ are constant matrices of appropriate dimensions.

As shown in Fig. 1, the plant contains N outputs $y_i(k)$ $(i = 1, 2, \ldots, N)$, which are spatially distributed [4, 14, 18]. Each output is attached to a sensor that is regarded as a slave station. At each sampling instant, the slave station can access the master station only when it holds the token. Fig. 2 shows the topological structure of the WICN, where the master station communicates with the slave station based on the token-based protocol.

Furthermore, WICN adopts Open System Interconnection (OSI) model that consists of several layers, such as Physical Layer (PL) and DLL, etc. DLL can be further divided into two sub-layers: Logical Link Control (LLC) and Media Access Control (MAC). In PL, all slave stations and the master station are designed based on IEEE 802.15.4a [23]. A traditional Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) protocol is used in MAC sub-layer to ensure the reliability of the data transmission. The token-based protocol is presented in the LLC sub-layer by two stages as follows:

1) Network generation. The master station incorporates the functioning and off-line slave stations into the token ring network. The off-line slave stations send "request network frame" to the master station. After being received, the connectivity table is constructed, as shown in Table 1. Every slave station has its own predecessor and successor. For instance, the

Table 1: Connectivity table

slave station	predecessor	successor
sensor 1	sensor N	sensor 2
sensor 2	sensor 1	sensor 3
$\vdots$	$\vdots$	$\vdots$
sensor N	sensor $N-1$	sensor 1

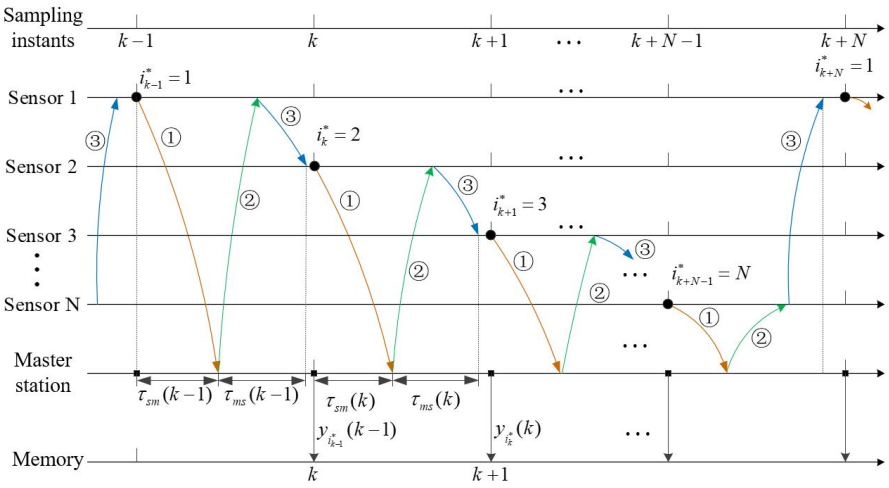

Fig. 3. Instance of timing diagram on the token-based protocol. ①: the data transmission. ②: the response frame transmission. ③: the token transmission.

first row in Table 1 illustrates sensor N and sensor 2 is the predecessor and successor of sensor 1, respectively. Then the master station encapsulates the connectivity table into "connection table frame" and sends it to all slave stations in the WICN. After sending "connection table frame", the master station enters the next stage: Network operation. Once the slave station receives "connection table frame", it records the predecessor as well as successor and stops sending "request network frame". Finally, the slave stations enter the following Network operation stage.

2) Network operation. Fig. 3 shows the detailed process of network operation. After sensor $i \in \{1, \ldots, N\}$ receives the token from its predecessor (shown as ③), it is activated. In other words, it takes a sample at the recent and right sampling instant k and transmits $y_i(k)$ to the master

station (shown as ① and the data transmission delay is $\tau_{sm}(k)$). Let $i_k^* \in \{1, \ldots, N\}$ denote the activated sensor at the sampling instant k, after the master station receives $y_{i_k^*}(k)$ at $k + \tau_{sm}(k)$, it immediately sends the response frame to sensor i_k^* (shown as ②). Then, after sensor i_k^* receives the response frame, it immediately sends the token to its successor where the token arrives at $k + \tau_{sm}(k) + \tau_{ms}(k)$ (shown as ③ and the sum of response frame as well as the token transmission delay is $\tau_{ms}(k)$).

Furthermore, the successor of sensor i_k^* is activated at $k+\lceil \tau_{sm}(k) + \tau_{ms}(k) \rceil$, where $\lceil \cdot \rceil$ represents that we round $\cdot$ up to the integer multiple of the sampling period. In practice, the update period of the sensor is generally less than $10ms$ [22, 46], and the whole time delay based on a modified IEEE 802.15.4 protocol is less than $10ms$ [2]. Here, we consider a typical case: $\lceil \tau_{sm}(k) + \tau_{ms}(k) \rceil = 1, \forall k \geqslant k_0$ (ensuring that the memory update instants are a step slower than the sensor sampling instants in the later simulation shown as Fig.7). Therefore, it can be seen obviously from Fig. 3 that sensor i_{k-1}^* and i_{k+1}^* are the predecessor and successor of sensor i_k^* respectively and the master station holds $y_{i_{k-1}^*}(k-1)$ at the sampling instant k.

Next, it is necessary to demonstrate clearly the value of each element in the memory attached to the master station at the sampling instant k. If the sampling data arrives, the data in the memory is used. It is different from the buffer where the data is used until all the needed data arrives [5]. We define a vector $\widehat{y}(k) = \left[\widehat{y}_1(k), \ldots, \widehat{y}_i(k), \ldots, \widehat{y}_N(k)\right]^T$ to describe all elements in the memory. After the master station receives $y_{i_{k-1}^*}(k-1)$, the corresponding element will be updated, i.e.,

$$\widehat{y}_i(k) = \begin{cases} y_{i_{k-1}^*}(k-1), i = i_{k-1}^*, \\ \widehat{y}_i(k-1), i \neq i_{k-1}^*. \end{cases} \tag{3}$$

Furthermore, a new quantity is introduced to express (3) as clearly as possible, i.e.,

$$\beta_i(k-1) = \begin{cases} 1, i = i_{k-1}^*, \\ 0, i \neq i_{k-1}^*. \end{cases} \tag{4}$$

Using (4), (3) can be re-written as

$$\widehat{y}_i(k) = \beta_i(k-1) y_i(k-1) + (1 - \beta_i(k-1))\, \widehat{y}_i(k-1). \tag{5}$$

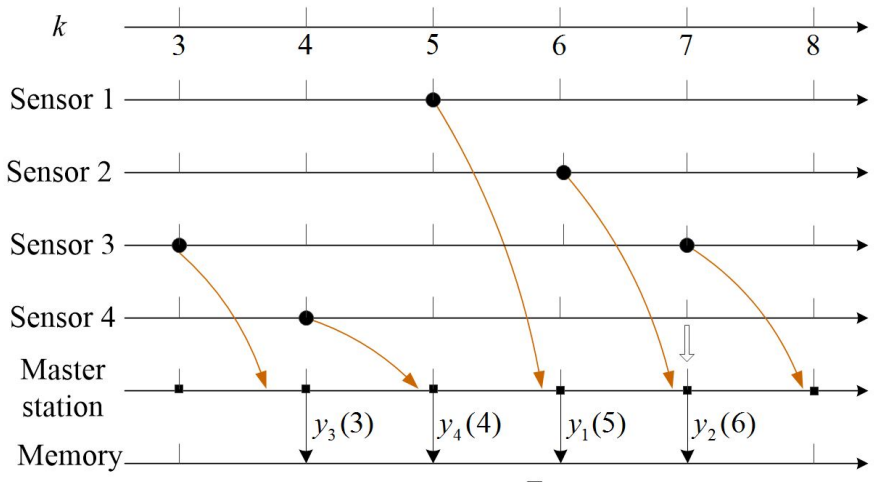

Fig. 4. Example of a wireless network with 4 sensors at the 7^{th} sampling instant : $\widehat{y}_2(7) = y_2(6)$; $\widehat{y}_3(7) = \widehat{y}_3(6) = \widehat{y}_3(5) = \widehat{y}_3(4) = y_3(3)$; $\widehat{y}_4(7) = \widehat{y}_4(6) = \widehat{y}_4(5) = y_4(4)$; $\widehat{y}_1(7) = \widehat{y}_1(6) = y_1(5)$.

Therefore, using (5), $\widehat{y}(k)$ can be expressed as

$$\widehat{y}(k) = \Lambda_{\sigma(k)} y(k-1) + \left(I - \Lambda_{\sigma(k)}\right) \widehat{y}(k-1), \tag{6}$$

where $\Lambda_{\sigma(k)} = diag\left\{\beta_1(k-1), \ldots, \beta_i(k-1), \ldots, \beta_N(k-1)\right\}$ denotes the updated components in the memory depending on $\sigma(k)$, and $\sigma(k)$ is defined by $\sigma(k) = i^*_{k-1},\ i^*_{k-1} \in \{1, \ldots, N\}$.

Remark 1. Note that, unlike *Theorem 2* in [25], the switching rule is preset as $\sigma(k) = i^*_{k-1}$ according to the token-based protocol, which can not be changed to stabilize the system. Meanwhile different from the traditional switched system, the number of sub-systems varies with deception attacks (to be discussed later).

To clearly show the data updates in the memory, Fig. 4 presents an instance of a wireless network with 4 sensors. It can be seen that at the 7^{th} sampling instant, sensor $i^*_7 = 3$ just holds the token but the master station keeps $y_{i^*_6}(6) = y_2(6)$. Thus, all elements in the memory are $\widehat{y}(7) = [y_1(5),\ y_2(6),\ y_3(3),\ y_3(4)]^T$.

Remark 2. The token-based wireless network is vulnerable in PL and DDL. For example, due to broadcast nature of the medium in PL [24, 34],

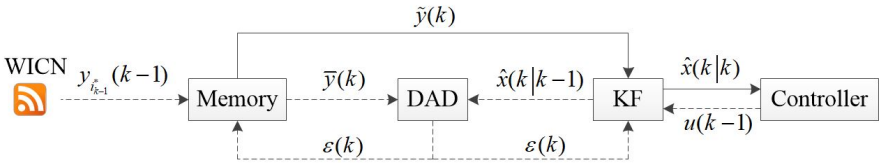

Fig. 5. Synergic action within DADCC. Dashed lines: action before detection. Solid lines: action after detection.

the attacker can access wireless network by breaking into the radio range of the slave stations or master station, and aims to inject the false data by distorting, relaying or replacing data packets. This destroys the authenticity of the original data.

2.2. Synergic action within DADCC

For the above token-based WICN, the data update process in the memory has been clearly analyzed. However, when wireless network is attacked, the authenticity of measurement data is destroyed. To detect deception attacks and repair the missing data, a synergic action within DADCC is conducted, as shown in Fig. 5. The action can be divided into the following two stages:

- Before detection: the memory is updated by the data received from the master station, becoming $\bar{y}(k)$, and the KF produces the *a priori* state estimation (i.e., $\hat{x}(k|k-1)$) based on the control signals (i.e., $u(k-1)$) at the previous sampling instant. Both will be sent to the deception attacks detector (DAD). Then using the pre-defined method, the DAD detects deception attacks and gives the detection result $\varepsilon(k)$.

- After detection: the memory is updated according to the detection result, becoming $\tilde{y}(k)$, which will be sent to the KF. Then the KF produces the *a posteriori* state estimation (i.e., $\hat{x}(k|k)$) according to the detection result. The estimation will be sent to the controller to generate the control signals at the current sampling instant k.

To clearly describe the above two stages, the pre-detection and post-detection measurements stored successively in the memory are firstly denoted by different forms, i.e., $\bar{y}(k) = [\bar{y}_1(k), \ldots, \bar{y}_i(k), \ldots, \bar{y}_N(k)]^T$ and $\tilde{y}(k) = [\tilde{y}_1(k), \ldots, \tilde{y}_i(k), \ldots, \tilde{y}_N(k)]^T$, respectively. At each sampling instant k, $\bar{y}(k)$

is updated by the measurements from master station and $\tilde{y}(k-1)$; $\tilde{y}(k)$ is updated by the detection result that decides whether the measurements from master station is used or not. Specially, $\tilde{y}(k) = \bar{y}(k)=\widehat{y}(k)$ if there are no deception attacks.

Next, the actions before detection (i.e., how to obtain the pre-detection measurements $\bar{y}(k)$, the *a priori* state estimation $\hat{x}(k|k-1)$ and the detection result $\varepsilon(k)$) are described as follows:

1) The pre-detection measurements $\bar{y}(k)$. At the sampling instant k, $y_{i^*_{k-1}}(k-1)$ from master station is used to update $\bar{y}_{i^*_{k-1}}(k)$ and other elements are updated by the corresponding elements from $\tilde{y}(k-1)$, i.e.,

$$\bar{y}_i(k) = \begin{cases} y_{i^*_{k-1}}(k-1), i = i^*_{k-1}, \\ \tilde{y}_i(k-1), i \neq i^*_{k-1}. \end{cases} \tag{7}$$

Using (4), (7) can be re-written as

$$\bar{y}_i(k) = \beta_i(k-1)y_i(k-1) + (1-\beta_i(k-1))\,\tilde{y}_i(k-1). \tag{8}$$

Thus, $\bar{y}(k)$ can be expressed as

$$\bar{y}(k) = \Lambda_{\sigma(k)}y(k-1) + \left(I - \Lambda_{\sigma(k)}\right)\tilde{y}(k-1), \tag{9}$$

where $\Lambda_{\sigma(k)}$ and $\sigma(k)$ are same as (6).

2) The *a priori* state estimation $\hat{x}(k|k-1)$. According to the idea of the standard KF in [3], $\hat{x}(k|k-1)$ is obtained by

$$\hat{x}(k\,|k-1) = A\hat{x}(k-1\,|k-1) + Bu(k-1). \tag{10}$$

3) The detection result $\varepsilon(k)$. Firstly, the pre-detection measurements $\bar{y}(k)$ and $\hat{x}(k\,|k-1)$ are used to produce the residual, i.e.,

$$z(k) = \bar{y}(k) - C\hat{x}(k\,|k-1). \tag{11}$$

To get the covariance of $z(k)$, according to the standard KF, the *a priori* estimation error covariance, the Kalman gain and the *a posteriori* estimation error covariance are given by

$$\begin{cases} P_{k|k-1} = AP_{k-1|k-1}A^T + Q, \\ G(k) = P_{k|k-1}C^T(CP_{k|k-1}C^T + R)^{-1}, \\ P_{k|k} = (I - G(k)C)P_{k|k-1}. \end{cases} \tag{12}$$

It is obvious that $P_{k|k-1}$ will converge from any initial condition [19], and the steady-state value denoted by $\tilde{P} = \lim_{k\to\infty} P_{k|k-1}$ can be obtained by the unique positive semi-definite solution of

$$\tilde{P} = A(\tilde{P} - \tilde{P}C^T(C\tilde{P}C^T + R)^{-1}C\tilde{P})A^T + Q. \tag{13}$$

The residual $z(k)$ is assumed as a white Gaussian process with zero mean and covariance $H = C\tilde{P}C^T + R$. Next, the DAD can be given by

$$h(k) = \sum_{s=k-\varsigma}^{k} z^T(s)H^{-1}z(s), \tag{14}$$

where $\varsigma \in \mathbb{Z}$. The DAD compares $h(k)$ with a pre-computed threshold ϑ. Once $h(k) > \vartheta$, a deception attack is assumed to be detected and the detection result $\varepsilon(k)$ is set as 0. Otherwise, $\varepsilon(k)$ is set as 1.

Furthermore, the actions after detection (i.e., how to obtain the post-detection measurements $\tilde{y}(k)$ and the *a posteriori* state estimation $\hat{x}(k|k)$) are given as follows:

1) The post-detection measurements $\tilde{y}(k)$. If $\varepsilon(k) = 1$, $y_{i^*_{k-1}}(k-1)$ is used to update $\tilde{y}_{i^*_{k-1}}(k)$. If $\varepsilon(k) = 0$, $\tilde{y}_{i^*_{k-1}}(k)$ holds the most recent value, i.e.,

$$\tilde{y}_i(k) = \begin{cases} \varepsilon(k)y_{i^*_{k-1}}(k-1) + (1-\varepsilon(k))\,\tilde{y}_{i^*_{k-1}}(k-1), i = i^*_{k-1}, \\ \tilde{y}_i(k-1), i \neq i^*_{k-1}. \end{cases} \tag{15}$$

Substituting (4) into (15), we have

$$\tilde{y}_i(k) = \varepsilon(k)\beta_i(k-1)y_i(k-1) + (1-\varepsilon(k)\beta_i(k-1))\,\tilde{y}_i(k-1). \tag{16}$$

Then, $\tilde{y}(k)$ can be expressed as

$$\tilde{y}(k) = M_{\tilde{\sigma}(k)}y(k-1) + \left(I - M_{\tilde{\sigma}(k)}\right)\tilde{y}(k-1), \tag{17}$$

where $M_{\tilde{\sigma}(k)} = \varepsilon(k)\Lambda_{\sigma(k)}$. Similar to (6), when $\varepsilon(k) = 1$, $M_{\tilde{\sigma}(k)}$ denotes the updated components of the post-detection measurements depending on $\tilde{\sigma}(k) = \sigma(k) = i^*_{k-1}$, and $\varepsilon(k) = 0$ prevents the update of the $(i^*_{k-1})^{th}$ component of the post-detection measurements in the memory. $\tilde{\sigma}(k)$ is defined by

$$\tilde{\sigma}(k) = \begin{cases} \sigma(k) = i^*_{k-1}, \quad if\ \varepsilon(k) = 1, \\ N+1, \quad if\ \varepsilon(k) = 0. \end{cases} \tag{18}$$

2) The *a posteriori* state estimation $\hat{x}(k|k)$. To simplify the following discussion, we assume that the KF in DADCC starts from the steady state, i.e., $P_{k_0|k_0-1} = \tilde{P}$, which leads to a steady-state KF with fixed gain $G = \tilde{P}C^T(C\tilde{P}C^T + R)^{-1}$ [19]. Then according to $\tilde{y}(k)$ and $\varepsilon(k)$, the *a posteriori* state estimation is obtained by

$$\hat{x}(k\,|k\,) = \hat{x}(k\,|k-1\,) + \varepsilon(k)G\left(\tilde{y}(k) - C\hat{x}(k\,|k-1\,)\right). \tag{19}$$

Remark 3. In general, if deception attacks happen, master station receives $y_{i^*_{k-1}}(k-1)$ injected with the false data so that the corresponding element in $\bar{y}(k)$ in (7) is discarded according to the detection result of the DAD in (14). Then, this missing data is reconstructed to compensate the corresponding element in $\tilde{y}(k)$ by using (15).

According to the above discussion, a new KF is obtained as follows:

$$\begin{cases} \hat{x}(k\,|k-1\,) = A\hat{x}(k-1\,|k-1\,) + Bu(k-1), \\ \hat{x}(k\,|k\,) = \hat{x}(k\,|k-1\,) + \varepsilon(k)G\left(\tilde{y}(k) - C\hat{x}(k\,|k-1\,)\right). \end{cases} \tag{20}$$

Remark 4. Compared with the traditional standard steady-state KF in [3], the proposed new KF incorporates compensation for the discarded data and detection results to handle deception attacks. Firstly, the ideal measurements in the standard steady-state KF are replaced by $\tilde{y}(k)$ in (20). If there exists the discarded data in $\bar{y}(k)$, it is reconstructed to compensate the corresponding element in $\tilde{y}(k)$ by using (15). Secondly, the detection result $\varepsilon(k)$ is incorporated into (20). When $\varepsilon(k) = 1$, (20) is degenerated into the standard steady-state KF; otherwise, $\hat{x}(k|k)$ is not updated.

According to $\hat{x}(k\,|k\,)$, a state feedback law can be designed as

$$u(k) = K\hat{x}(k\,|k\,). \tag{21}$$

Substituting (17) and (21) into (20), it follows that

$$\begin{aligned} \hat{x}(k\,|k\,) = D_{\tilde{\sigma}(k)}\hat{x}(k-1\,|k-1\,) + E_{\tilde{\sigma}(k)}Cx(k-1) \\ +F_{\tilde{\sigma}(k)}\tilde{y}(k-1) + E_{\tilde{\sigma}(k)}v(k-1), \end{aligned} \tag{22}$$

where $\tilde{\sigma}(k)$ is same as (17), $D_{\tilde{\sigma}(k)} = \left(I - \varepsilon(k)GC\right)(A + BK)$, $E_{\tilde{\sigma}(k)} = \varepsilon(k)GM_{\tilde{\sigma}(k)}$, $F_{\tilde{\sigma}(k)} = \varepsilon(k)G\left(I - M_{\tilde{\sigma}(k)}\right)$.

Consequently, substituting (21) and (22) into (1), we can obtain a closed-loop system

$$\begin{aligned} x(k+1) = Ax(k) + \tilde{D}_{\tilde{\sigma}(k)}\hat{x}(k-1\,|k-1) + \tilde{E}_{\tilde{\sigma}(k)}Cx(k-1) \\ +\tilde{F}_{\tilde{\sigma}(k)}\tilde{y}(k-1) + \tilde{E}_{\tilde{\sigma}(k)}v(k-1) + w(k), \end{aligned} \tag{23}$$

where $\tilde{D}_{\tilde{\sigma}(k)} = BKD_{\tilde{\sigma}(k)}$, $\tilde{E}_{\tilde{\sigma}(k)} = BKE_{\tilde{\sigma}(k)}$, $\tilde{F}_{\tilde{\sigma}(k)} = BKF_{\tilde{\sigma}(k)}$, $\tilde{\sigma}(k)$ defined in (17) is such a function $\tilde{\sigma} : [k_0, \infty) \to J = \{1, \ldots, N+1\}$, which denotes the switching function. Denote

$$\{(j_0, s_0), (j_1, s_1), \ldots, (j_m, s_m), \ldots | s_0 = k_0, m \in \mathbb{Z}, j_m \in J\}$$

as the switching rule, where $\tilde{\sigma}(k) = j_m$ means that the sub-system j_m locates in $[s_m, s_{m+1})$. The switching instants series $\{s_m\}$ is the subsequence of the sampling instants series $\{k\}$, i.e., $\{s_m\} \subseteq \{k\}$.

Remark 5. For the closed-loop system (23), the system structure firstly becomes more complex. This is because the sub-system $1, \ldots, N$ may switch based on the token-based protocol, but an additional new sub-system $N+1$ is induced under deception attacks. On the other hand, the parameters of the system are also more complex because the post-detection measurements $\tilde{y}(k)$ and the detection result $\varepsilon(k)$ are incorporated into (23). Therefore, it is more difficult to analyze the stability of WNCSs compared with that of NCSs [38, 43–45].

2.3. Control objectives

We are interested in how to make sure that WNCSs are robust under deception attacks. Two control objectives are considered here: one is the duration of deception attacks; another is the associated stability and system performance.

Definition 1-Sub-system Duration [35]. Considering any sampling instant k or l, and $k \geqslant l \geqslant k_0$, $\Theta_j(l, k)$ denotes the duration of the sub-system j in $[l, k)$, where $j \in J$. Then there are $\kappa \in \mathbb{N}$ and $\theta_j \leqslant 1$ satisfying

$$\Theta_j(l, k) \leqslant \kappa + (k - l)\theta_j, \tag{24}$$

where $\Theta_{N+1}(l, k)$ can be called deception attacks duration. Moreover, the incident rate θ_j of the sub-system j satisfies

$$\sum_{j \in J} \theta_j = 1. \tag{25}$$

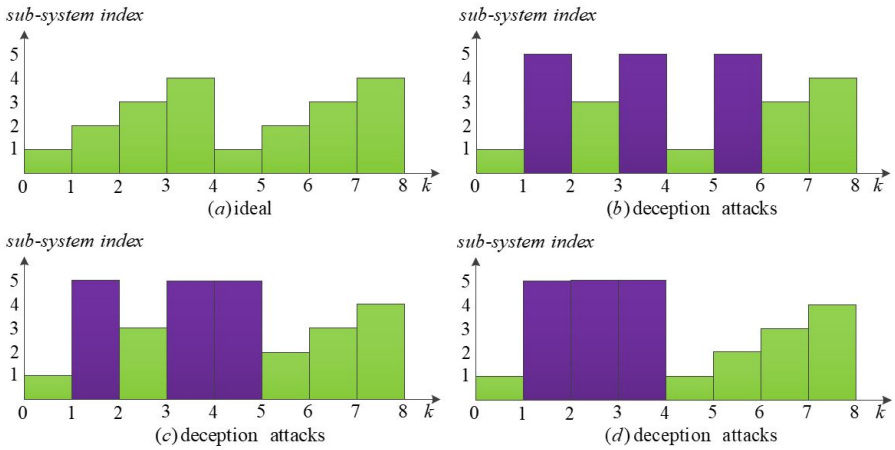

Fig. 6. Instances of deception attacks with 4 sensor nodes. (a): ideal WNCSs with sub-systems $1, 2, 3, 4$. (b): deception attacks induce sub-system 5 in [1,2), [3,4) and [5,6). (c): deception attacks induce sub-system 5 in [1,2) and [3,5). (d): deception attacks induce sub-system 5 in [1,4).

Especially, θ_{N+1} is called the incident rate of deception attacks.

Remark 6. The definition of *sub-system duration* extends that of *DoS duration* in [35] since the system under no deception attack is a switched system due to the token-based protocol. Further, by using (24), we can get θ_{N+1} according to θ_i as discussed in the following Definition 3.

Inequality (24) and equation (25) can be explained in Fig. 6. For example, to calculate the sub-system duration with 4 sensor nodes, Fig. $6(a)$ yields: $\Theta_1(0,8) = \Theta_2(0,8) = \Theta_3(0,8) = \Theta_4(0,8) = 2, \Theta_5(0,8) = 0$, $\theta_1 = \theta_2 = \theta_3 = \theta_4 = 1/4, \theta_5 = 0$; Fig. $6(b)$ yields: $\Theta_1(0,8) = 2$, $\Theta_2(0,8) = 0$, $\Theta_3(0,8) = 2$, $\Theta_4(0,8) = 1$, $\Theta_5(0,8) = 3$, $\theta_1 = 1/4$, $\theta_2 = 0$, $\theta_3 = 1/4$, $\theta_4 = 1/8$, $\theta_5 = 3/8$.

Another important point, the switching numbers have the connection with the sub-system duration.

Definition 2-Switching numbers [13]. Considering any sampling instant k or l, and $k \geqslant l \geqslant k_0$, $n(l,k)$ represents the switching numbers of switching signal $\tilde{\sigma}(k)$ in $[l,k)$. Then there are $N_0 \in \mathbb{N}$ and $T \in \mathbb{R}$ satisfying:

$$n(l,k) \leqslant N_0 + (k-l)/T. \tag{26}$$

Lemma 1-Connection between deception attacks and switching numbers. Considering the same notation in Definitions 1 and 2, when

deception attacks appear, T and the incident rate of deception attacks θ_{N+1} satisfy

$$\theta_{N+1} > 1 - 1/T \tag{27}$$

for all $k > k_0$.

Proof. When deception attacks are absent, we have $\{s_m\} = \{k\}, n(l,k) = k - l$; however, under deception attacks, we have $\{s_m\} \subseteq \{k\}, n(l,k) \leqslant (k-l)/T$, where $m \in \mathbb{Z}$, $k > l \geqslant k_0$, $T \geqslant 1$, $N_0 = 0$. Thus, it can be seen clearly that deception attacks can reduce $n(l,k)$. Denote the reduction of $n(l,k)$ by

$$\Delta n(l,k) = k - l - n(l,k).$$

Meanwhile, deception attacks produce the sub-system $N+1$. Thus, the relationship between $\Theta_{N+1}(l,k)$ and $\Delta n(l,k)$ can be given by

$$\Theta_{N+1}(l,k) > \Delta n(l,k). \tag{28}$$

Using (24) and (26), (27) can be obtained from (28). The proof is ended.

Fig. 6 explains the inequality (27). For instance, to calculate the duration of deception attacks and the switching numbers with 4 sensor nodes, Fig. 6(b),(c),(d) all yields: $\Theta_5(0,8) = 3$; Meanwhile Fig. 6(b),(c),(d) yields: $\Delta n(0,8) = 0$, $\Delta n(0,8) = 1$, $\Delta n(0,8) = 2$, respectively. It can be seen that the duration of deception attacks is always greater than the reduction of the switching numbers.

Furthermore, the following definition is provided to prove the exponential stability of the closed-loop system.

Definition 3. Consider any deception attacks sequences satisfying Definitions 1 and 2 such that

$$\theta_{N+1} \leqslant \theta'_{N+1} = f(\theta_i), \tag{29}$$

where $i = 1, \ldots, N$. Then the system (23) is exponentially stable with a noise level index $\lambda > 0$, i.e.,

(1) For $v(k)$ and $w(k)$, there is

$$|x(k)| > \lambda \sup\left(|v(q-1) + w(q)|\right), \forall q \geqslant k_0, \tag{30}$$

where $|\circ|$ means the Euclidean norm of $\circ$.

(2) When $v(k) \equiv 0$ and $w(k) \equiv 0$, there exist $c > 0$ and decay rate $\rho > 1$ such that the solutions of the system (23) satisfy

$$|x(k)| \leqslant c\rho^{-(k-k_0)} |x(k_0)| \tag{31}$$

for all $k > k_0$.

Remark 7. Referring to [11, 15, 25, 35], Definition 3 is given for analyzing the stability of token-based WNCSs under deception attacks. It mainly contains three aspects: 1) Similar as an admissible maximum communication denial on the average in [35], a condition of maximum allowable incident rate of deception attacks is presented. 2) Similar as the given filtering performance in [11, 15, 25], a noise level is provided for $v(k)$ and $w(k)$. 3) Referring to [25], an exponential stability condition is given when $v(k) \equiv 0$ and $w(k) \equiv 0$.

3. Stability analysis

The characters of the above closed-loop switched system have been analyzed, including the sub-system duration, the switching numbers and the connection between deception attacks and switching numbers. In this section, the exponential stability with a noise level index is proved and the maximum allowable duration of deception attacks is obtained to maintain the exponential stability of the system.

Theorem 1. Consider the closed-loop switched system (23), if the tuning parameters $a_i > 1,\ a_{N+1} < 1,\ \mu > 1,\ \theta_i \leqslant 1,\ \theta_{N+1} \leqslant 1,\ i = 1, 2, \ldots, N$, $\lambda > 0$, the matrices $P_{pj} \in \mathbb{R}^{n_x \times n_x},\ p = 1, 2, 3, 4, j \in J$ should satisfy

$$\Phi_j < 0, \tag{32}$$

$$P_{pj} \leqslant \mu P_{pq}, p = 1, 2, 3, 4, j \neq q \in J, \tag{33}$$

where

$$\begin{aligned}\Phi_j = {} & \phi_{1j}^T P_{1j} \phi_{1j} + \phi_{2j}^T P_{2j} \phi_{2j} + \phi_{3j}^T P_{3j} \phi_{3j} + \phi_{4j}^T P_{4j} \phi_{4j} \\ & - a_j^{-2} \phi_{5j}^T P_{1j} \phi_{5j} - a_j^{-2} \phi_{6j}^T P_{2j} \phi_{6j} - a_j^{-2} \phi_{7j}^T P_{3j} \phi_{7j} - a_j^{-2} \phi_{8j}^T P_{4j} \phi_{8j} \\ & + \lambda^{-1} \phi_{5j}^T \phi_{5j} - \lambda \phi_{9j}^T \phi_{9j} - \lambda \phi_{10j}^T \phi_{10j},\end{aligned}$$

$$\phi_{1j} = \left[\begin{array}{ccccc} A & \tilde{D}_j & \tilde{E}_j & \tilde{F}_j & \tilde{E}_j \end{array} \quad I_{n_x\times n_x}\right],$$
$$\phi_{2j} = \left[\begin{array}{ccccc} 0_{n_x\times n_x} & D_j & E_j & F_j & E_j \end{array} \quad I_{n_x\times n_x}\right], \phi_{3j} = \left[\begin{array}{cc} C & 0_{n_x\times 5n_x} \end{array}\right],$$
$$\phi_{4j} = \left[\begin{array}{ccccc} 0_{n_x\times 2n_x} & M_j & I_{n_x\times n_x} - M_j & M_j & 0_{n_x\times n_x} \end{array}\right],$$
$$\phi_{5j} = \left[\begin{array}{cc} I_{n_x\times n_x} & 0_{n_x\times 5n_x} \end{array}\right], \phi_{6j} = \left[\begin{array}{ccc} 0_{n_x\times n_x} & I_{n_x\times n_x} & 0_{n_x\times 4n_x} \end{array}\right],$$
$$\phi_{7j} = \left[\begin{array}{ccc} 0_{n_x\times 2n_x} & I_{n_x\times n_x} & 0_{n_x\times 3n_x} \end{array}\right], \phi_{8j} = \left[\begin{array}{ccc} 0_{n_x\times 3n_x} & I_{n_x\times n_x} & 0_{n_x\times 2n_x} \end{array}\right],$$
$$\phi_{9j} = \left[\begin{array}{ccc} 0_{n_x\times 4n_x} & I_{n_x\times n_x} & 0_{n_x\times n_x} \end{array}\right], \phi_{10j} = \left[\begin{array}{cc} 0_{n_x\times 5n_x} & I_{n_x\times n_x} \end{array}\right],$$

$I_{n_x\times n_x}$ is the $n_x \times n_x$ real identity matrix, then the system is exponentially stable with decay rate $\rho = \mu^{-1/2T}\left(\prod_{j=1}^{N+1} a_j^{\theta_j}\right)$ under the maximum allowable incident rate of deception attacks, i.e., θ'_{N+1}, satisfying

$$\theta_{N+1} \leqslant \theta'_{N+1} = (\ln\sqrt{\mu} - \sum_{i=1}^{N}\theta_i \ln a_i) \Big/ (\ln\sqrt{\mu} + \ln a_{N+1}). \tag{34}$$

Proof. Choosing the following Lyapunov function:

$$\begin{aligned} V_{\tilde{\sigma}(k)}(k) = {} & x^T(k)P_{1\tilde{\sigma}(k)}x(k) + \hat{x}^T(k-1\,|k-1)P_{2\tilde{\sigma}(k)}\hat{x}(k-1\,|k-1) \\ & + x^T(k-1)C^T P_{3\tilde{\sigma}(k)}Cx(k-1) + \tilde{y}^T(k-1)P_{4\tilde{\sigma}(k)}\tilde{y}(k-1). \end{aligned} \tag{35}$$

To derive easily, two quantities are denoted by

$$\xi(k) = \left[x^T(k)\ \hat{x}^T(k-1\,|k-1)\ x^T(k-1)C^T\ \tilde{y}^T(k-1)\ v^T(k-1)\ w^T(k)\right]^T$$

and $\Gamma(k) = \lambda^{-1}x^T(k)x(k) - \lambda v^T(k-1)v(k-1) - \lambda w^T(k)w(k)$.

The following proof is performed in two cases.

1) When $k \in [s_m, s_{m+1}^-)$, $\tilde{\sigma}(k) = \tilde{\sigma}(k+1) = j_m$, which indicates that no switch occurs, it follows from (35) and (32) such that

$$\begin{aligned} & V_{\tilde{\sigma}(k+1)}(k+1) - a_{\tilde{\sigma}(k)}^{-2}V_{\tilde{\sigma}(k)}(k) + \Gamma(k) \\ & = V_{j_m}(k+1) - a_{j_m}^{-2}V_{j_m}(k) + \Gamma(k) \\ & = \xi^T(k)\Phi_{j_m}\xi(k) < 0. \end{aligned} \tag{36}$$

Thus, we can derive $V_{j_m}(k)$ from $V_{j_m}(s_m)$ such that

$$\begin{aligned} V_{j_m}(k) & < a_{j_m}^{-2}V_{j_m}(k-1) - \Gamma(k-1) \\ & < a_{j_m}^{-2\times 2}V_{j_m}(k-2) - a_{j_m}^{-2}\Gamma(k-2) - \Gamma(k-1) \\ & < \dots \\ & < a_{j_m}^{-2\times(k-s_m)}V_{j_m}(s_m) - \Omega_1(k), \end{aligned} \tag{37}$$

where

$$\Omega_1(k) = \sum_{q=s_m}^{k-1} a_{j_m}^{-2(k-1-q)}\Gamma(q).$$

2) When $k = s_m$, the sub-system $\tilde{\sigma}(k^-) = j_{m-1}$ switches to the sub-system $\tilde{\sigma}(k) = j_m$, where $j_{m-1} \neq j_m \in J$, we can derive $V_{j_m}(k)$ from $V_{j_{m-1}}(k^-)$ by using (33) such that

$$V_{j_m}(k) \leqslant \mu V_{j_{m-1}}(k^-). \tag{38}$$

Furthermore, using the above (37) and (38), we can derive $V_{j_m}(k)$ from $V_{j_0}(s_0)$ such that

$$\begin{aligned} V_{j_m}(k) &< a_{j_m}^{-2(k-s_m)} V_{j_m}(s_m) - \Omega_1(k) \\ &< \mu^{n(s_{m-1},s_m)} a_{j_m}^{-2(k-s_m)} a_{j_{m-1}}^{-2(s_m^- - s_{m-1})} V_{j_{m-1}}(s_{m-1}) \\ &\quad -\mu^{n(s_{m-1},s_m)} a_{j_m}^{-2(k-s_m)} \Omega_1(s_m^-) - \Omega_1(k) \\ &< \dots \\ &< \mu^{n(s_0,s_m)} a_{j_m}^{-2(k-s_m)} \dots a_{j_0}^{-2(s_1^- - s_0)} V_{j_0}(s_0) - \Omega_2(k) \\ &= \mu^{n(s_0,k)} \prod_{j=1}^{N+1} a_j^{-2\Theta_j(s_0,k)} V_{j_0}(s_0) - \Omega_2(k), \end{aligned} \tag{39}$$

where

$$\Omega_2(k) = \sum_{r=1}^{m} \mu^{n(s_{r-1},s_m)} \prod_{j}^{N+1} a_j^{-2\Theta_j(s_r,k)} \Omega_1(s_r^-) + \Omega_1(k),$$

$$\prod_{j=1}^{N+1} a_j^{-2\Theta_j(s_r,k)} = a_{j_m}^{-2(k-s_m)} \dots a_{j_r}^{-2(s_{r+1}^- - s_r)}, r \in \{0, 1, \dots, m\}.$$

To further analyze (39), the following two steps are carried out.

i) Consider the second term at its right, i.e.,

$$\begin{aligned} \Omega_2(k) = &\sum_{r=1}^{m} \mu^{n(s_{r-1},s_m)} \prod_{j}^{N+1} a_j^{-2\Theta_j(s_r,k)} \sum_{q=s_m}^{s_r^- - 1} a_{j_r}^{-2(s_r^- - 1 - q)} \Gamma(q) \\ &+ \sum_{q=s_m}^{k-1} a_{j_m}^{-2(k-1-q)} \Gamma(q) > 0. \end{aligned} \tag{40}$$

To make (40) hold, we need

$$\begin{aligned}&\Gamma(q)\\&=\lambda^{-1}x^T(q)x(q)-\lambda v^T(q-1)v(q-1)-\lambda w^T(q)w(q)>0,\end{aligned}\tag{41}$$

where $q \geqslant s_0$. Thus, we obtain

$$|x(k)|>\lambda \sup\left(|v(q-1)+w(q)|\right), \forall q \geqslant s_0 \tag{42}$$

for $k \geqslant k_0$.

ii) According to (39) and (40), the first term at its right follows that

$$V_{j_m}(k)<\mu^{n(s_0,k)}\prod_{j=1}^{N+1}a_j^{-2\Theta_j(s_0,k)}V_{j_0}(s_0). \tag{43}$$

Then we further analyze the relationship between the parameters in (43) and the stability of the whole switched system. The performance of each sub-system should be discussed, i.e.,

1) For each sub-system, if there are $a_i^{-2}<1, a_{N+1}^{-2}>1$, it means that the sub-system i is stable and the sub-system $N+1$ is unstable, where $i=1,\ldots,N$.

2) For each switching action, there is $\mu>1$. This means that the switching action degrades the performance of the closed-loop system.

If the above two cases hold, we can obtain

$$\begin{aligned}V_{j_m}(k)&<\mu^{(k-s_0)/T}\left(\prod_{j=1}^{N+1}a_j^{\theta_j}\right)^{-2(k-s_0)}V_{j_0}(s_0)\\&<\rho^{-2(k-s_0)}V_{j_0}(s_0)\\&=\rho^{-2(k-k_0)}V_{j_0}(k_0),\end{aligned}\tag{44}$$

where $\rho=\mu^{-1/2T}\left(\prod_{j=1}^{N+1}a_j^{\theta_j}\right)$.

Here, if (44), (42) and (34) hold, it indicates that $\rho = \mu^{-1/2T}\left(\prod_{j=1}^{N+1} a_j^{\theta_j}\right) > 1$, i.e., $\sum_{j=1}^{N+1} \theta_j \ln a_j > (1/T)\ln\sqrt{\mu}$, it guatantees the exponential stability of the closed-loop switched system (23). This completes the proof.

Remark 8. Specially, if the parameters a_i, μ and λ in Theorem 1 are set as $a_i > 1$, $\mu > 1$ and $\lambda > 0$, it actually describes the system performance under no deception attacks, i.e., $\theta_{N+1} = 0$.

However, we do not always know all incident rates of sub-system i. Hence, the following corollary also presents the results for the case where all incident rates of sub-system i are unified.

Corollary 1. Consider the closed-loop switched system (23), if we have the tuning parameters $a_i = a_1 > 1,\ a_{N+1} < 1,\ \mu > 1,\ \theta_i \leqslant 1,\ \theta_{N+1} \leqslant 1,\ i = 1,\ 2,\ \ldots,\ N,\ \lambda > 0$, and the matrices $P_{pj} \in \mathbb{R}^{n_x \times n_x},\ p = 1, 2, 3, 4, j \in J$ satisfy (32) and (33), the system is exponentially stable with decay rate $\rho = \mu^{-1/2T} a_1^{1-\theta_{N+1}} a_{N+1}^{\theta_{N+1}}$ under the maximum allowable incident rate of deception attacks, i.e., θ'_{N+1}, satisfying

$$\theta_{N+1} \leqslant \theta'_{N+1} = (\ln\sqrt{\mu} - \ln a_1)/(\ln\sqrt{\mu} + \ln a_{N+1} - \ln a_1). \tag{45}$$

Proof. Choosing the same Lyapunov function as (35) and using (32) and (33), we can obtain (39). Then we choose a noise level index to satisfy (40). According to (39) and (40), (43) is obtained. Similarly, by the analysis of the parameters in (43) and using (25), we have

$$V_{j_m}(k) < \rho^{-2(k-k_0)} V_{j_0}(k_0), \tag{46}$$

where $\rho = \mu^{-1/2T} a_1^{1-\theta_{N+1}} a_{N+1}^{\theta_{N+1}}$. For all sub-systems, if $a_i = a_1, a_i \neq a_{N+1}$ and $\rho > 1$, it follows that

$$\theta_{N+1} \leqslant ((1/T)\ln\sqrt{\mu} - \ln a_1)/(\ln a_{N+1} - \ln a_1). \tag{47}$$

Furthermore, from Lemma 1 and (47), we can obtain (45).

Remark 9. The inequalities (34) and (45) both provide the upper bound, i.e., the maximum allowable incident rate θ'_{N+1} of deception attacks. However, when the sub-systems and network environment are similar, the tuning parameters a_i can be set as the same values. Since $\sum_{j\in J} \theta_j = 1$ in (25), (34) becomes the simpler form (45). This can be easier to calculate.

4. Simulation

Assume that an inverted pendulum system has four sensors for measuring its cart displacement, velocity, pendulum angle and angular velocity. The parameters of the discrete-time system model are expressed as:

$$A = \begin{bmatrix} 1.0000 & 0.0100 & 0 & 0 \\ 0 & 0.9993 & -0.0059 & 0 \\ 0 & 0 & 1.0016 & 0.0100 \\ 0 & 0.0022 & 0.3109 & 1.0016 \end{bmatrix}, B = \begin{bmatrix} 0 \\ 0.0074 \\ -0.0001 \\ -0.0222 \end{bmatrix}, C = I_{4\times 4},$$

$$Q = diag\{0.00001, 0.00001, 0.00001, 0.00001\},$$
$$R = diag\{0.00001, 0.00001, 0.00001, 0.00001\}.$$

Deception attacks may deteriorate the system performance even cause the system instability, and so do the noises. If the covariance matrices of the noises are set as very large values, it will further accelerate the deterioration of system performance. To more clearly show how the proposed approach to handle deception attacks, the small Q and R are chosen.

The sampling period is $10ms$, and the closed-loop system can be stabilized under LQR gain $K = \begin{bmatrix} 3.1194 & 6.2077 & 57.3024 & 14.2449 \end{bmatrix}$. Then, we choose the system parameters as listed in Table 2. According to these system parameters and the controller, $T^{'} = 1.0714$ and the maximum allowable incident rate $\theta_5^{\prime}$ of deception attacks is 6.77%. The initialization parameters of the system and steady-state KF are set as

$$x(k_0) = \begin{bmatrix} 0 & 0 & 0.02 & 0 \end{bmatrix}^T, \hat{x}(k_0 - 1\,|k_0 - 1) = \begin{bmatrix} 0 & 0 & 0.02 & 0 \end{bmatrix}^T,$$

$$G = \begin{bmatrix} 0.6180 & 0.0011 & 0 & 0 \\ 0.0011 & 0.6179 & 0 & 0 \\ 0 & 0 & 0.6151 & 0.0328 \\ 0 & 0 & 0.0328 & 0.6282 \end{bmatrix},$$

where $k_0 = 3$. The token-based protocol is shown in Fig. 7.

Next, the attack instants and the injected false data are presented in Table 3. The detection function is expressed as (14), where $k \geqslant k_0 + 2$,$\varsigma = 3$. When there exist no deception attacks, $h(k)$ is shown in Fig. 8.

However, if there exist deception attacks, we obtain $h(k)$ as shown in Fig. 9. The incident rate θ_5 of deception attacks is 6.02%.

Table 2: System parameters

tuning parameters	impact of the switching actions	noise level index
$a_1 = a_2 = a_3 = a_4 = 1.0010$, $a_5 = 0.9870$	$\mu = 1.0001$	$\lambda = 0.8500$

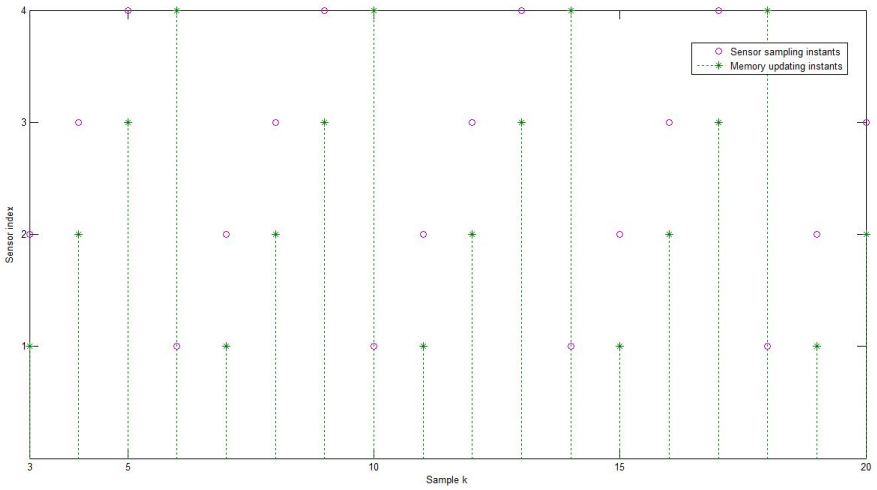

Fig. 7. Token-based protocol.

Table 3: Attack instants and the injected false data

attack instant	injected false data	attack instant	injected false data
40	$[\ 0\ \ 0.2\ \ 0\ \ 0\ ]^T$	540	$[\ 0\ \ 0.2\ \ 0\ \ 0\ ]^T$
88	$[\ 0\ \ 0.2\ \ 0\ \ 0\ ]^T$	595	$[\ 0.2\ \ 0\ \ 0\ \ 0\ ]^T$
154	$[\ 0\ \ 0\ \ 0\ \ 0.2\ ]^T$	624	$[\ 0\ \ 0.2\ \ 0\ \ 0\ ]^T$
167	$[\ 0.2\ \ 0\ \ 0\ \ 0\ ]^T$	690	$[\ 0\ \ 0\ \ 0\ \ 0.2\ ]^T$
242	$[\ 0\ \ 0\ \ 0\ \ 0.2\ ]^T$	727	$[\ 0.2\ \ 0\ \ 0\ \ 0\ ]^T$
268	$[\ 0\ \ 0.2\ \ 0\ \ 0\ ]^T$	799	$[\ 0.2\ \ 0\ \ 0\ \ 0\ ]^T$
312	$[\ 0\ \ 0.2\ \ 0\ \ 0\ ]^T$	848	$[\ 0\ \ 0.2\ \ 0\ \ 0\ ]^T$
387	$[\ 0.2\ \ 0\ \ 0\ \ 0\ ]^T$	869	$[\ 0\ \ 0\ \ 0.2\ \ 0\ ]^T$
429	$[\ 0\ \ 0\ \ 0.2\ \ 0\ ]^T$	937	$[\ 0\ \ 0\ \ 0.2\ \ 0\ ]^T$
479	$[\ 0.2\ \ 0\ \ 0\ \ 0\ ]^T$	986	$[\ 0\ \ 0\ \ 0\ \ 0.2\ ]^T$

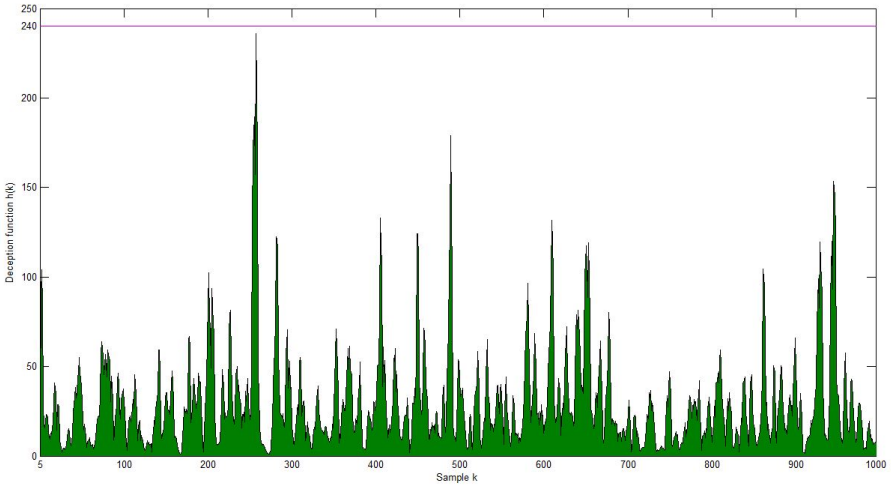

Fig. 8. Detection function $h(k)$ in the absence of deception attacks.

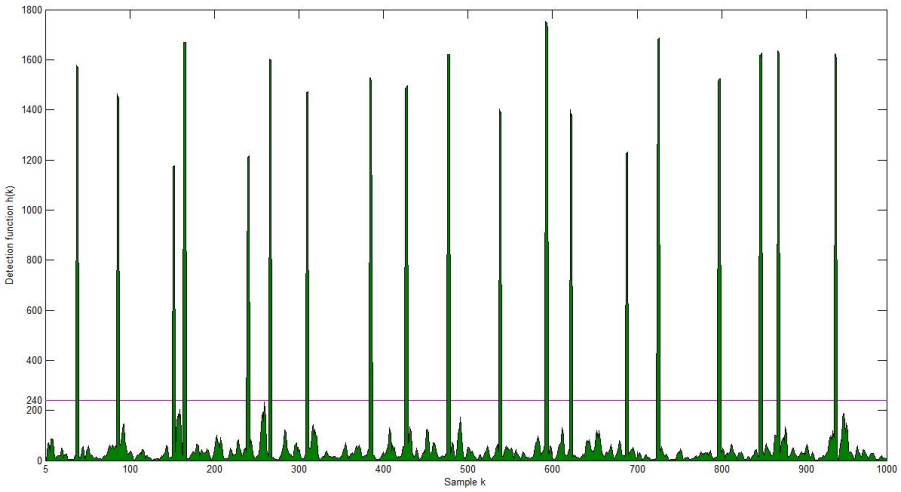

Fig. 9. Detection function $h(k)$ in the presence of given deception attacks.

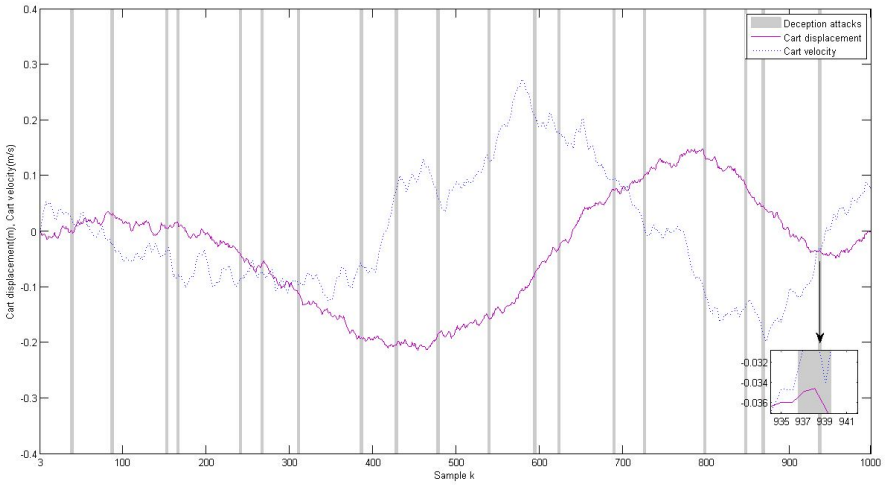

Fig. 10. State curves of cart displacement and cart velocity.

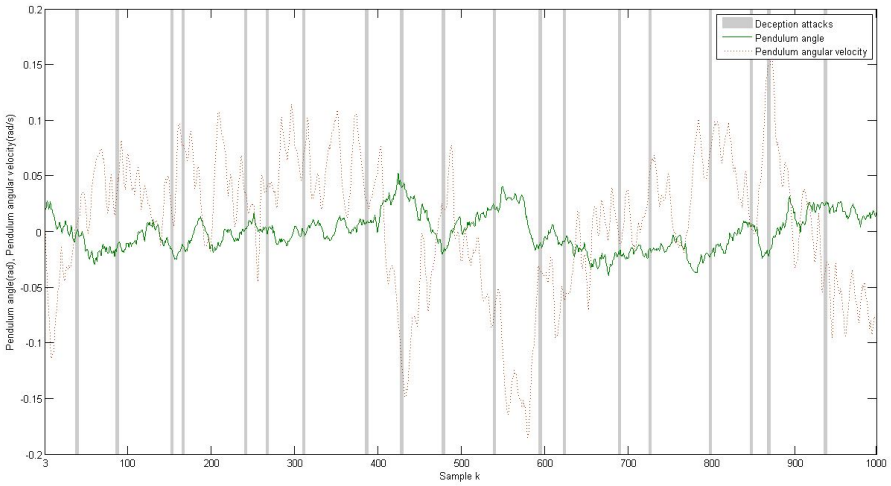

Fig. 11. State curves of pendulum angle and pendulum angular velocity.

Finally, the state of the inverted pendulum system is shown in Figs. 10 and 11. The system is stable under $\theta_5 = 6.02\% < \theta_5' = 6.77\%$. Moreover, we can also obtain

$$\begin{aligned} |x(k)| &\geqslant \inf\left(|x(q)|\right) = 0.0164 \\ &> \lambda \sup\left(|v(q-1) + w(q)|\right) = 0.8500 \times 0.0190 = 0.01615. \end{aligned}$$

This confirms the effectiveness of the proposed approach.

5. Conclusion

The paper has investigated the stability of token-based WNCSs under deception attacks. Firstly, with respect to the token-based protocol applied to the DLL, an innovative switched system model is developed, where the number of sub-systems will be changed under deception attacks. Then, a new KF scheme is proposed for attack detection and the missing data reconstruction. Furthermore, for the given linear feedback WNCSs, when the noise level is below a threshold derived, the maximum allowable duration of deception attacks is obtained to maintain the exponential stability of the system. Future work may involve the consideration of WNCSs under hybrid attacks and the corresponding method to cope with these hybrid attacks.

Acknowledgments

This work was supported in part by the National Science Foundation of China (Nos. 61473182, 61773253, 61633016, 61533010). The Key Project of Science and Technology Commission of Shanghai Municipality (Nos. 15220710400, 15JC1401900)

References

[1] S. Amin, X. Litrico, S. Sastry, A.M. Bayen, Cyber security of water SCADA systemspart I: Analysis and experimentation of stealthy deception attacks, IEEE Trans. Control Syst. Technol. 21(5) (2013) 1963-1970.

[2] M. Anwar, Y. Xia, Y. Zhan, TDMA-based IEEE 802.15.4 for low-latency deterministic control applications, IEEE Trans. Ind. Informat. 12(1) (2016) 338-347.

[3] C. Bai, V. Gupta, F. Pasqualetti, On kalman filtering with compromised sensors: attack stealthiness and performance bounds, IEEE Trans. Autom. Control 62(12) (2017) 6641-6648.

[4] L. Ding, Q.-L. Han, X. Ge, X. Zhang, An overview of recent advances in event-triggered consensus of multiagent systems, IEEE Trans. Cybern. 48(4) (2018) 1110-1123.

[5] L. Ding, Q.-L. Han, G. Guo, Network-based leader-following consensus for distributed multi-agent systems, Automatica 49(7) (2013) 2281-2286.

[6] L. Ding, Q.-L. Han, L. Wang, E. Sindi, Distributed cooperative optimal control of DC microgrids with communication delays, IEEE Transactions on Industrial Informatics. (2018) DOI: 10.1109/TII.2018.2799239.

[7] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, X. Zhang, A survey on security control and attack detection for industrial cyber-physical systems, Neurocomputing 275 (2018) 1674-1683.

[8] D. Ding, Z. Wang, Q.-L. Han, G. Wei, Security control for discrete-time stochastic nonlinear systems subject to deception attacks, IEEE Transactions on Systems, Man, and Cybernetics: Systems. (2016) DOI: 10.1109/TSMC.2016.2616544.

[9] S.X. Ding, P. Zhang, S. Yin, E.L. Ding, An integrated design framework of fault-tolerant wireless networked control systems for industrial automatic control applications, IEEE Trans. Ind. Informat. 9(1) (2013) 462-471.

[10] D. Du, R. Chen, X. Li, L. Wu, P. Zhou, M. Fei, Malicious data deception attacks against power systems: A new case and its detection method, Transactions of the Institute of Measurement and Control. (2018) DOI: 10.1177/0142331217740622.

[11] D. Du, B. Qi, M. Fei, C. Peng, Multiple event-triggered H_2/H_∞ filtering for hybrid wired-wireless networked systems with random network-induced delays, Inf. Sci. 325 (2015) 393-408.

[12] D. Du, B. Qi, M. Fei, Z. Wang, Quantized control of distributed event-triggered networked control systems with hybrid wired-wireless networks communication constraints, Inf. Sci. 380 (2017) 74-91.

[13] Z. Fei, S. Shi, Z. Wang, L. Wu, Quasi-time dependent output control for discrete-time switched system with mode-dependent average dwell time, IEEE Transaction Automatic Control. (2017) DOI: 10.1109/TAC.2017.2771373.

[14] D. Freirich, E. Fridman, Decentralized networked control of systems with local networks: A time-delay approach, Automatica 69 (2016) 201-209.

[15] X. Ge, Q.-L. Han, Distributed event-triggered H_∞ filtering over sensor networks with communication delays, Inf. Sci. 291 (2015) 128-142.

[16] X. Ge, Q.-L. Han, Consensus of multiagent systems subject to partially accessible and overlapping Markovian network topologies, IEEE trans. Cybern. 47(8) (2017) 1807-1819.

[17] X. Ge, Q.-L. Han, F. Yang, Event-based set-membership leader-following consensus of networked multi-agent systems subject to limited communication resources and unknown-but-bounded noise. IEEE Trans. Ind. Electron. 64(6) (2017) 5045-5054.

[18] X. Ge, F. Yang, Q.-L. Han, Distributed networked control systems: A brief overview, Inf. Sci. 380 (2017) 117-131.

[19] Z. Guo, D. Shi, K.H. Johansson, L. Shi, Optimal linear cyber-attack on remote state estimation, IEEE Trans. Control Netw. Syst. 4(1) (2017) 4-13.

[20] W. Hou, Y. Song, H. Wang, A. Hunger, Architecture and performance of the industrial wired/wireless hybrid networks with multi-token, in: Proceding of the 3rd ACM Workshop Mobile Sensing, Computing and Communication, 2016, pp. 7-15.

[21] L. Hu, Z. Wang, Q.-L. Han, X. Liu, State estimation under false data injection attacks: Security analysis and system protection, Automatica 87 (2018) 176-183.

[22] IEEE Computer Society, IEEE standard for local and metropolitan area networks–part 15.4: Low-rate wireless personal area networks (LR-WPANs) amendment 1: MAC sublayer, IEEE Std 802.15.4e-2012 (Amendment to IEEE Std 802.15.4-2011), 2012.

[23] E. Karapistoli, F.N. Pavlidou, I. Gragopoulos, I. Tsetsinas, An overview of the IEEE 802.15.4a standard, IEEE Commun. Mag. 48(1) (2010) 47-53.

[24] D. Lecompte, F. Gabin, Evolved multimedia broadcast/multicast service (eMBMS) in LTE-advanced: Overview and Rel-11 enhancements, IEEE Commun. Mag. 50(11) (2012) 68C74.

[25] J. Lian, C. Li, D. Liu, Input-to-state stability for discrete-time non-linear switched singular systems, IET Control Theory Appl. 11(16) (2017) 2893-2899.

[26] L. Ma, Z. Wang, Q.-L. Han, H.K. Lam, Variance-constrained distributed filtering for time-varying systems with multiplicative noises and deception attacks over sensor networks, IEEE Sensors J. 17(7) (2017) 2279-2288.

[27] Y. Mo, B. Sinopoli, On the performance degradation of cyber-physical systems under stealthy integrity attacks, IEEE Trans. Autom. Control 61(9) (2016) 2618-2624.

[28] E. Moradi-Pari, H.N. Mahjoub, H. Kazemi, Y.P. Fallah, A. Tahmasbi-Sarvestani, Utilizing model-based communication and control for cooperative automated vehicle applications, IEEE Trans. Intell. Veh. 2(1) (2017) 38-51.

[29] M. Mozaffari, W. Saad, M. Bennis, M. Debbah, Wireless communication using unmanned aerial vehicles (UAVs): Optimal transport theory for hover time optimization, IEEE Trans. Wireless Commun. 16(12) (2017) 8052-8066.

[30] C. Peng, S. Ma, X. Xie, Observer-based non-PDC control for networked T-S fuzzy systems with an event-triggered Communication, IEEE Trans. Cybern. 47(8) (2017) 2279 - 2287.

[31] C. Peng, M. Wu, X. Xie, Y. Wang, Event-triggered predictive control for networked nonlinear systems with imperfect premise matching, IEEE Transaction on Fuzzy Systems. (2018) DOI : 10.1109/TFUZZ.2018.2799187.

[32] C. Peng, J. Zhang, Q.-L. Han, Consensus of multi-agent systems with nonlinear dynamics using an integrated sampled-data-based event-triggered communication scheme, IEEE Transactions on Systems, Man, and Cybernetics: Systems. (2018) DOI: 10.1109/TSMC.2018.2814572.

[33] C. Peng, J. Zhang, H. Yan, Adaptive event-triggering H_∞ load frequency control for network-based power systems, IEEE Trans. Ind. Electron. 65(2) (2018) 1685-1694.

[34] A. Perrig, J. Stankovic, D. Wagner, Security in wireless sensor networks, Commun. ACM 47(6) (2004) 53C57.

[35] C.D. Persis, P. Tesi, Input-to-state stabilizing control under denial-of-service, IEEE Trans. Autom. Control 60(11) (2015) 2930-2944.

[36] M. Raza, N. Aslam, H. Le-Minh, S. Hussain, Y. Cao, N.M. Khan, A critical analysis of research potential, challenges and future directives in industrial wireless sensor networks, IEEE Communications Surveys & Tutorials. (2017) DOI: 10.1109/COMST.2017.2759725.

[37] W. Shen, T. Zhang, F. Barac, M. Gidlund, PriorityMAC: A priority-enhanced MAC protocol for critical traffic in industrial wireless sensor and actuator networks, IEEE Trans. Ind. Informat. 10(1) (2014) 824-835.

[38] Q. Sun, C.C. Lim, P. Shi, F. Liu, Design and stability of moving horizon estimator for markov jump linear systems, IEEE Transactions on Automatic Control. (2018) DOI: 10.1109/TAC.2018.2816102.

[39] F. Tramarin, S. Vitturi, M. Luvisotto, A dynamic rate selection algorithm for IEEE 802.11 industrial wireless LAN, IEEE Trans. Ind. Informat. 13(2) (2017) 846-855.

[40] Y. Wang, S.X. Ding, D. Xu, B. Shen, An H_∞ fault estimation scheme of wireless networked control systems for industrial real-time applications, IEEE Trans. Control Syst. Technol. 22(6) (2014) 2073-2086.

[41] M. Wu, L. Tan, N. Xiong, Data prediction, compression, and recovery in clustered wireless sensor networks for environmental monitoring applications, Inf. Sci. 329(2016) 800-818.

[42] W. Yang, L. Lei, C. Yang, Event-based distributed state estimation under deception attack, Neurocomputing 270 (2017) 145-151.

[43] X. Zhang, Q.-L. Han, Network-based H_∞ filtering using a logic jumping-like trigger, Automatica 49(5) (2013) 1428-1435.

[44] X. Zhang, Q.-L. Han, X. Yu, Survey on recent advances in networked control systems, IEEE Trans. Ind. Informat. 12(5) (2016) 1740-1752.

[45] B. Zhang, Q.-L. Han, X. Zhang, Event-triggered H_∞ reliable control for offshore structures in network environments, Journal of Sound and Vibration 368 (2016) 1-21.

[46] R. Zurawski, From wireline to wireless networks and technologies, IEEE Trans. Ind. Informat. 3(2) (2007) 93-94.